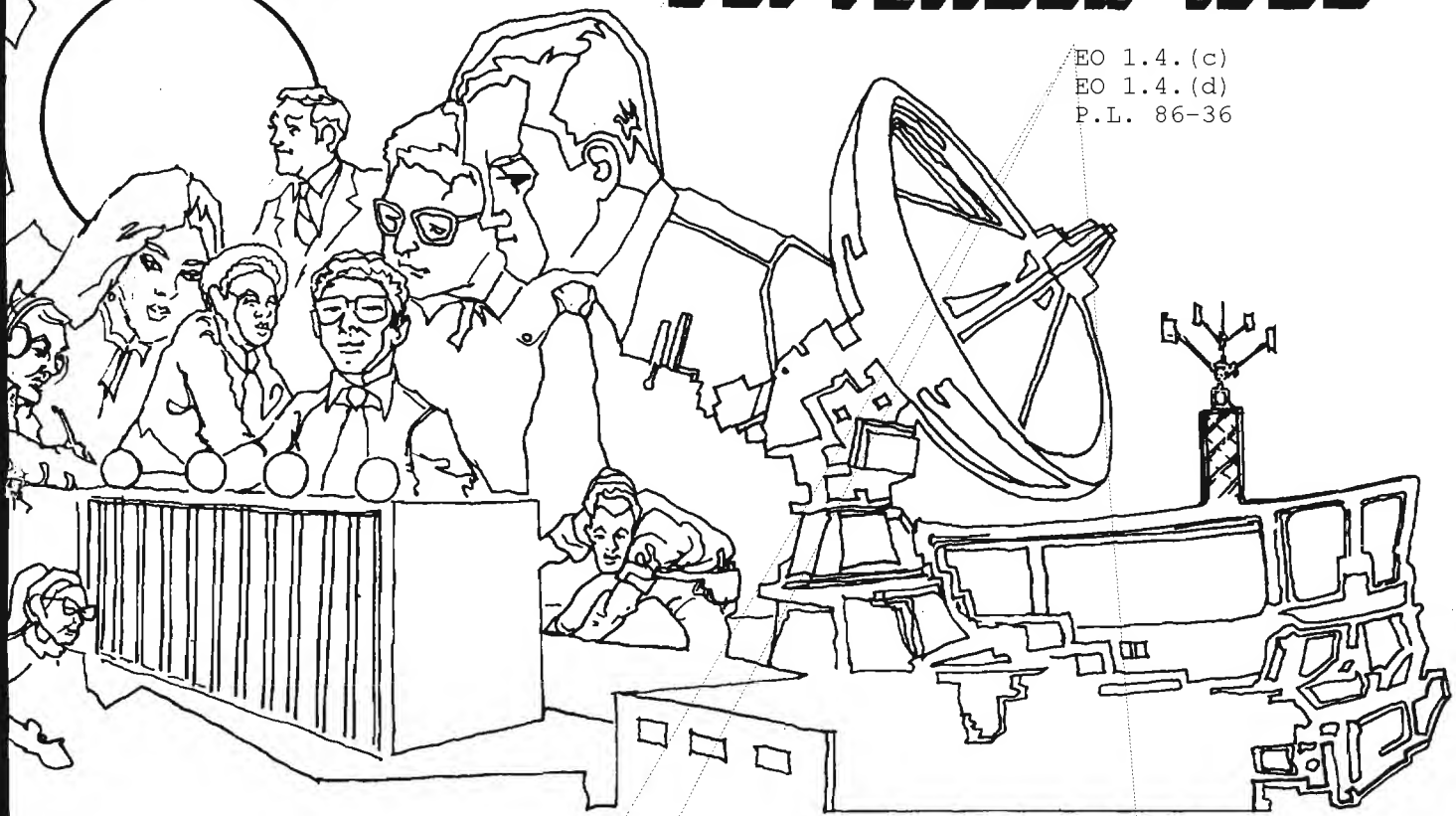
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1983



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 9 SEPTEMBER 1983

For subscriptions
send name and organization

to: [redacted] P14
(963-3369s)

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at bar1cØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Editorial

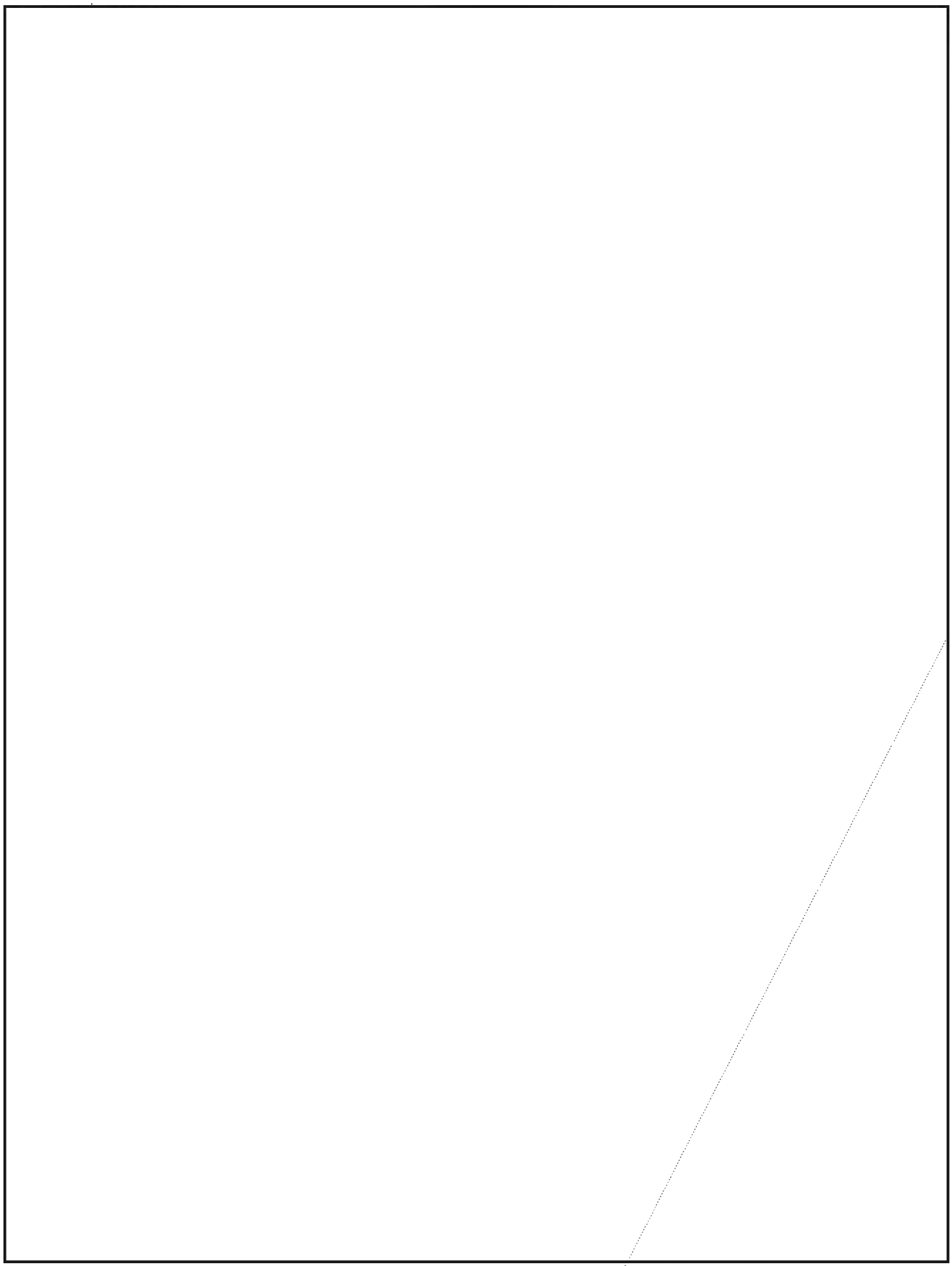
In a nearby university, so the story goes, there was a professor of Marine Biology who was almost legendary for his inability to remember any of the names of his students. He did not even remember the names of his graduate students. One day the Dean asked him, "How is it that you can never remember the names of your students?" "I learned long ago," the professor replied, "that each time I remember the name of a student, I forget the name of a fish."

Our business around here is, at the heart, an intellectual activity. We work at understanding and solving various complex processes and problems, many of which are intentionally devious and difficult.

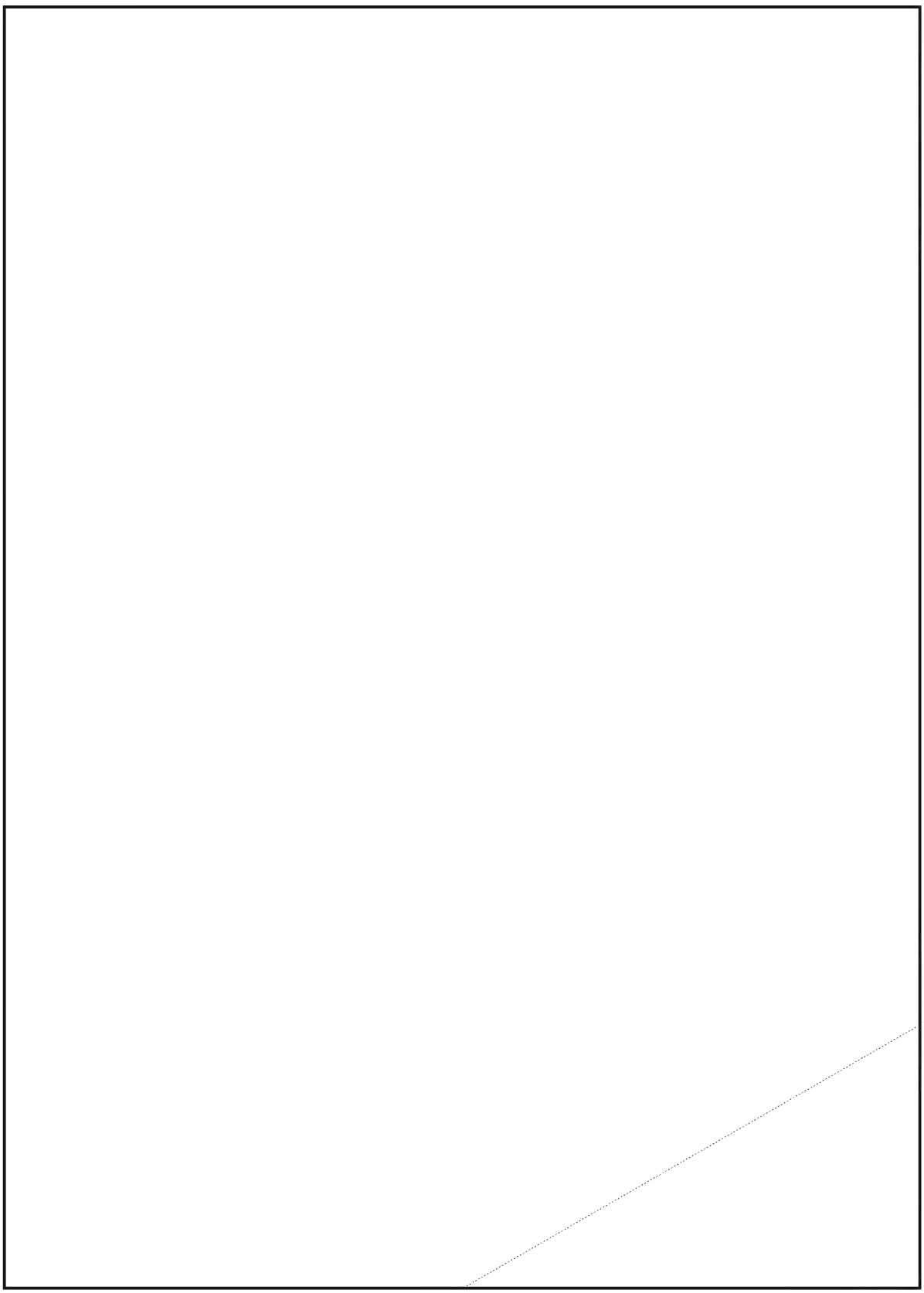
Our system of managing the resources to do all this needs a lot of "fine tuning" (a favorite word of managers) so that the taxpayers, who pay for all of this, will get their money's worth. That is a good and necessary goal, but sometimes our zeal for "fine tuning" produces complicated and bureaucratic mazes that are more efficient in appearance than in substance.

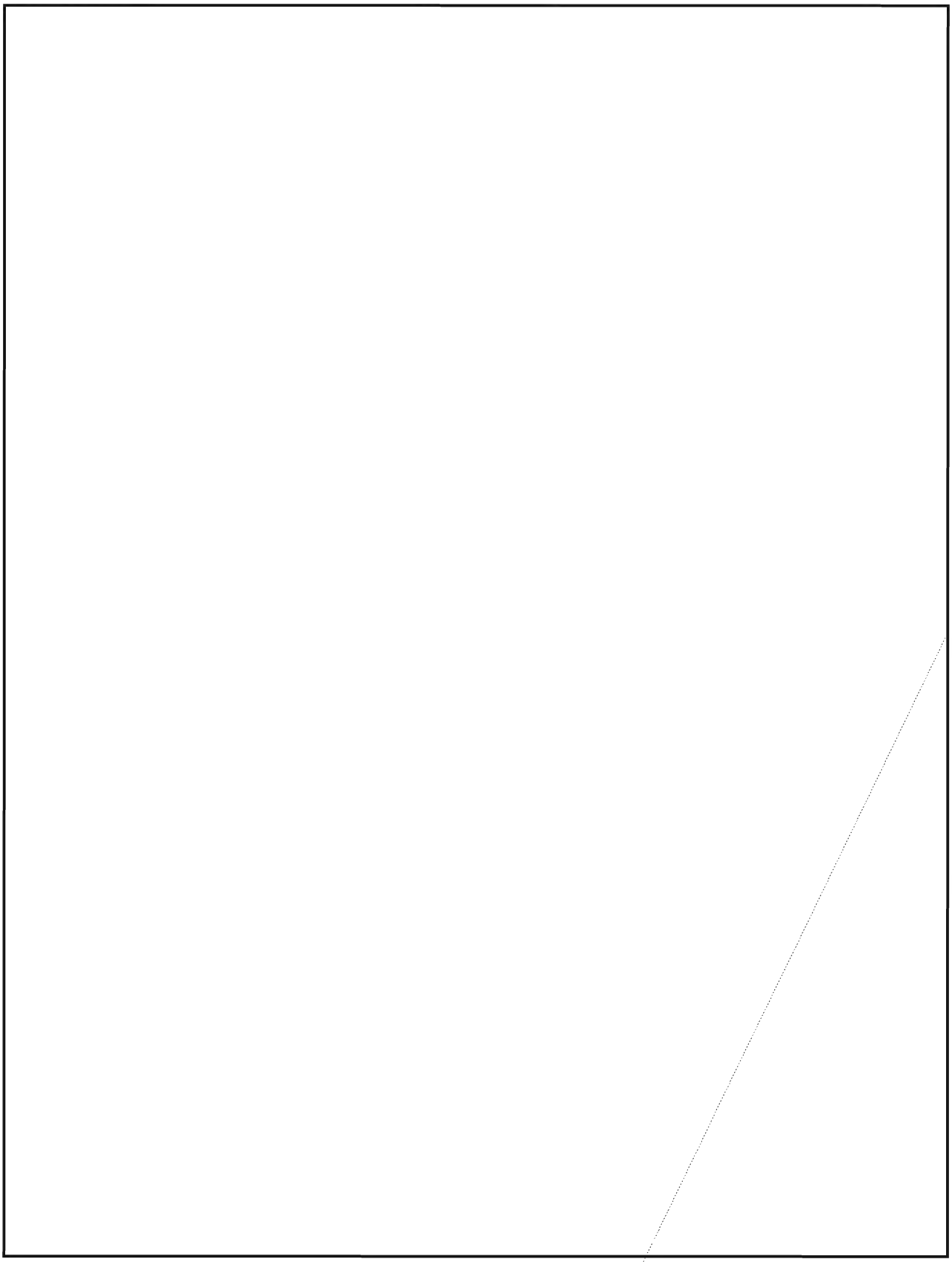
It is all very well to say that we should be smart enough to operate under "sophisticated" organizations and "fine tuned" coordination procedures. And it is also true that most analytic people can, if they turn their minds to it, understand and operate within the most complex operating systems.

Each of us in the analytic business, like the professor, begins each day with only so much "analytic energy" and the more of that energy we spend trying to understand our system--the less we have left over to spend on the target we sometimes call the enemy.

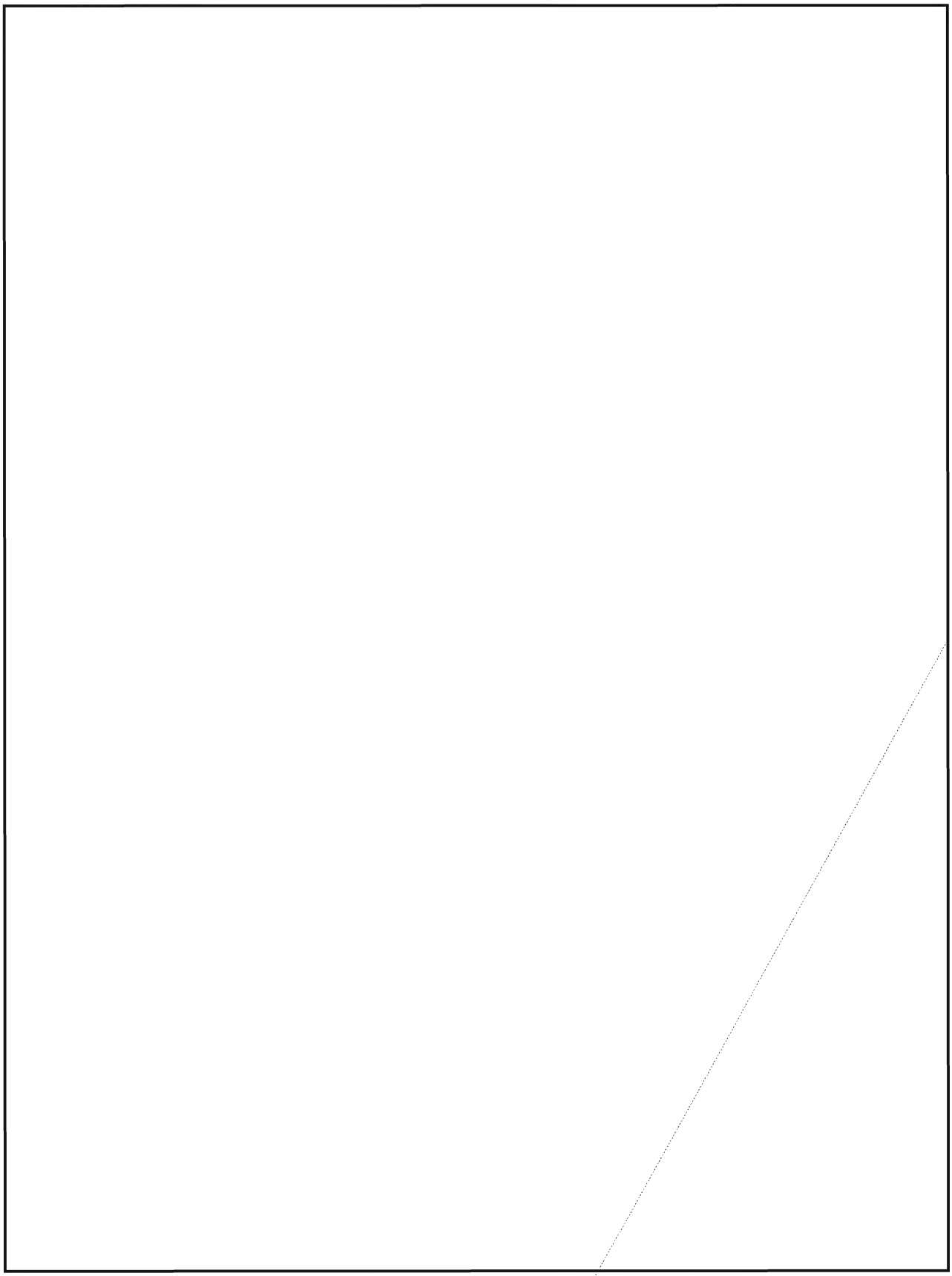


EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

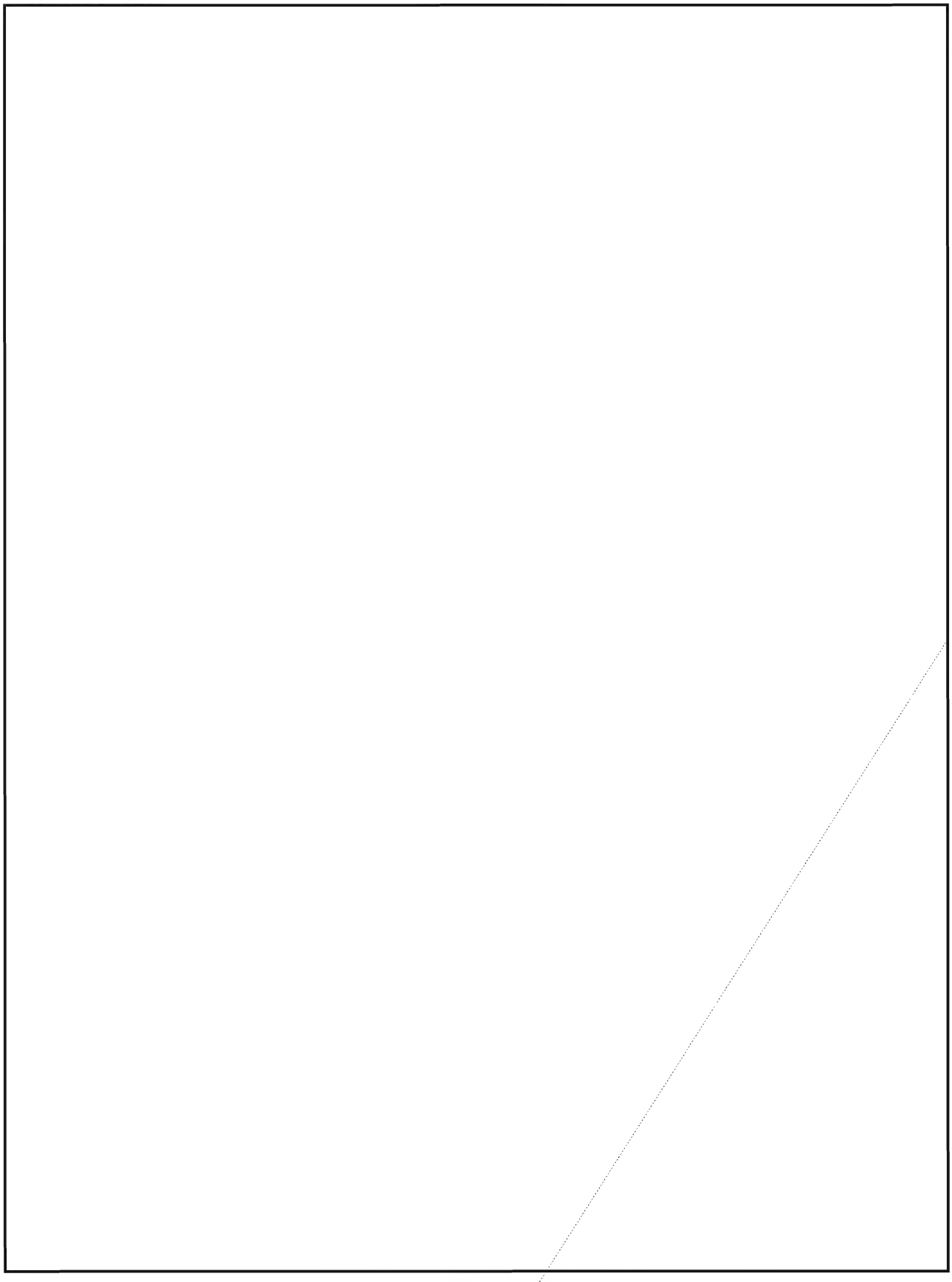




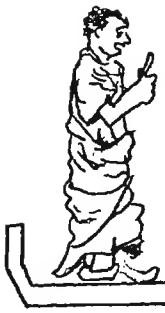
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



Do You Really Mean JULIAN?

by [redacted] P13

P.L. 86-36

The Data Standards Center (P13D) recently established a new data standard: DE 00105 Ordinal Day The data chain Ordinal Date is of course already a standard, DE 00013. It consists of Year (2N), followed directly by Ordinal Day; e.g.,"83109" to represent 19 April 1983.

If Ordinal Date is already a standard, why worry about one of its components, Ordinal Day? Well, as most NSA people involved in data processing well know, the latter for many years has wrongly been mislabeled "Julian Day." In fact a few years ago, NSA electrical messages used to include a space for entering "Julian Day." Fortunately with the help of sympathetic staff people within T, the NDSC was able to lobby against "Julian Day" so persistently that the term was finally expunged from NSA/CSS electrical message formats. It felt like a major victory!

Accordingly, it now seems appropriate to make "Ordinal Day" an official standard to help lay the ghost of "Julian Day" finally to rest, although that may be easier said than done!

"Julian Date" of course has been equally as persistent as "Julian Day" as a ubiquitous misnomer. Indeed, one of the main reasons for standardizing "Ordinal Date" was to give us some ammunition for suppressing "Julian Date." Incidentally, the ISO (International Standards Organization) has standardized Ordinal Date (ISO 2711), following action by the American National Standards Institute (ANSI) in 1971 to also standardize calendar date and ordinal dates. Both ANSI and the ISO use the term "day of the year" for the data element that encompasses the ordinal days. However, we felt that "Ordinal Day" is perhaps more descriptive of the data element itself.

"Julian Day" and "Julian Date" are of course valid terms, but not in the way that NSA has sometimes employed them. The following information from the Encyclopaedia Britannica summarizes the proper use of these two interlopers.

[] JULIAN DATE: The term "Julian Date" refers to a date taken from the Julian Calendar (named for Julius Caesar) that is at present 13 days behind our standard Gregorian Calendar (named for Pope Gregory XIII).

Joseph Justus Scaliger

(1540-1609)

[] JULIAN DAY The concept of numbering days in one-up order is derived from the "Julian Period" system, primarily used by astronomers. (This system was devised by Joseph Scaliger in the 16th century as a universal measure of chronology and named for his father, not for the Roman emperor, although his father, Julius Caesar Scaliger, had been named after the emperor.) "Julian Days" are not numbered one-up through the year, as are "Ordinal Days," but rather throughout the "Julian Period" of 7,980 years that began with Day 1 starting at noon on 1 January 4731 BC (Julian Calendar) and will end at noon on 1 January 3268 AD Julian (which will be 23 January Gregorian) with day 2,914,695.

So you can see neither term represents what quite a few of us NSA people thought it did.

Julius Caesar Scaliger

(1484-1558)

WHAT IS THIS THING CALLED

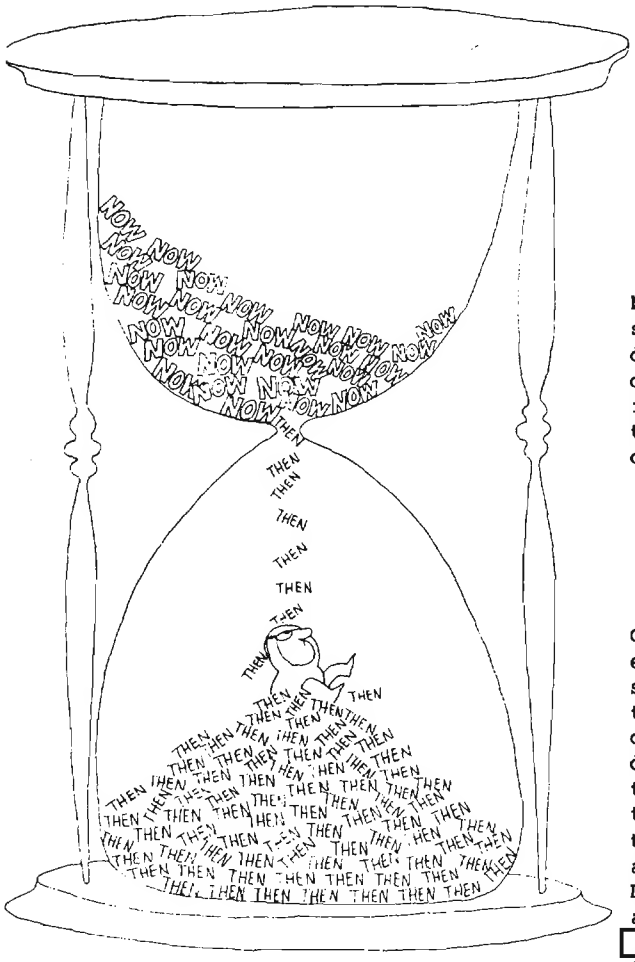
"an undefined medium in which existing objects appear to develop irreversibly in the changes which they undergo, and in which events and phenomena appear to occur in succession."

The use of "appear to" probably satisfies both physicists and philosophers. However, such a definition would drive a data standardizer right up the wall! In the data standards world, precision and accuracy are premium items, and definitions have to be right to the point. Note, for example, the standard definition for DE 00017, Time:

"An expression of a specific hour and minute of the 24-hour period of the calendar day "

One cannot enjoy the luxury of philosophy, etc., when faced with the demands of a data standard! The above illustrates the point that the definition of a term, and that of a corresponding data standard (if any), can differ to a considerable degree. By the way, the NDSC has a big investment also in SIGINT terminology as well as data standards. The terminology team in P13D has already published authoritative glossaries on Traffic Analysis, Direction Finding, and SIGINT Collection, as annexes to USSID 412. Contact [redacted] (on 968-8161s) for information about any of the above.

P.L. 86-36



MANAGEMENT OF COORDINATION (U)

by [redacted]
Captain, USAF
JOCCP

(U) The three little words that always make me cringe are "Coordinate this please." Coordination is really time-consuming and, if taken in regular doses, has got to be the main cause of nervous breakdowns among Agency employees.

Webster's definition of "coordination" includes the word "harmonious" but real staff coordination is anything but that. "Acrimonious" would be more appropriate. I often take a deep breath before walking into an office with a piece of "For Coordination" correspondence that appears controversial. I don't think that anything is as frustrating as wandering the equivalent of five miles through a labyrinth of hallways to get three small initials on a piece of paper. No, wait! I can think of something even more frustrating.

You walk around those hallways searching out the final office chief to get him/her to put the final "blessing" on your (by now) cannibalized (otherwise known as "edited") product and he/she disagrees with the whole principle of the paper and tells you that he/she will not concur. ("I non-concur," is usually the expression used.) I sometimes would give my right arm for one of two things in this type of situation:

[] a pistol (preferably one of high caliber) or

[] a high tree (with a conveniently placed strong horizontal limb) and a strong rope.

It would not be extremely disappointing to receive one or two "suggested changes," but each "coordinatee" has his/her own method of inserting these "recommendations." Each one has an unmistakable style, but they can usually be divided into three basic categories:

1. The "arrow maker," who usually goes around placing arrows below (or above or in the margin near) the sentence or word in question. (Sometimes I would like to suggest where to put some of those arrows and now I know why Custer got it in the end.)

2. The inimitable user of Xs, who uses rather large Xs to blot out whole paragraphs, sometimes destroying continuity and making your paper look something like a cross (pun intended!) between a fingerpainting by a mentally disturbed kindergarten student and a colony of eartheworms making love to one another. (The best remedy for X-makers is to provide a pen for them to use, making sure that it is a very soft felt-tip marker--which frustrates their editing--or a pen just about ready to run out of ink. This intimidation process may hamper their efforts and they may give up in disgust, telling you that your paper is fine.)

3. The "thinker," who sits there and ponders the paper, regardless of whether it is a two-liner or a two-pager) and corrects grammar ("It's 'you and I,' not 'you and me'!") or spelling ("There are only two Os in 'coordinate'!"). The best way to counter the thinker is to put several "one-dollar" words in the paper - the best one being "propinquity." This word isn't often used in Agency papers and the "coordinatee" may take one of two actions when

confronted with it: He/she may try to show knowledge of the word thereby forcing immediate agreement to the point in which the term appears; or he/she may take the time to look it up (or possibly ask you for a definition in the hope that you really don't know), thereby disrupting his/her thought processes. (Of course, nothing from nothing is nothing.) By the way, "propinquity" means "nearness."

The following main points are absolutely essential when embarking on a coordination trek:

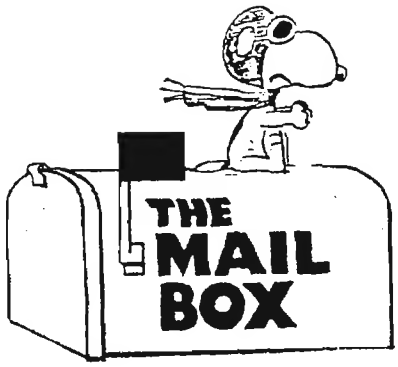
1. HAVE AN OPEN MIND. Be as objective as possible when someone edits your paper, even when you are thinking about ripping your hair out or applying cattle prods to the other person's anatomy;

2. ALWAYS BE AGREEABLE TO CHANGE. If you fight editing changes, this may lead to more "pen massacre" on your work. (It's similar to when your father or or mother used to catch you doing wrong: If you argued, the paddle seemed lighter and hurt more.)

3. KEEP YOUR COOL! Leaning over the desk and breaking the editor's pen, glasses, nose, or arm may make you feel better, but it certainly will not solve the problem. Besides, you can't get initials from a person in intensive care. (Refer to Rule #2 in such cases.)

4. REMEMBER THAT MURDER IS POSSIBLY PUNISHABLE BY DEATH. Except in this case where the charge may be reduced to justifiable manslaughter.

If you keep these rules in mind, coordination will be as much fun for you as it is for the many inmates of Sing Sing or the patients at Saint Elizabeths. Just remember that, if all else fails, your mother always liked you--but she never had to put her initials on anything you wrote.



Dear Sir:

I read with interest the article in the June/July 1983 issue of CRYPTOLOG entitled REDBARON, ROADRUNNER, & BRONZSTAR: What's in a Name? The article points out a problem that this organization has been struggling with for some time. That is the attempt to educate project officers within the Agency about NSA/CSS Regulation No. 10-5, Assignment and Handling of Cover Terms.

This regulation states that approval to use covernames must be obtained from the NSA Cover Term Officer (CTO) who determines the eligibility of specific words for use as covernames. It also states that covernames of similar or related type will not be assigned to projects or operations that are themselves similar or related. Nor will they be a term that will tend to reveal the meaning of the activity (e.g., abbreviations or acronyms).

Not going by the rules in the assignment of covernames can lead to compromise of not only one project but a whole series of projects if they are not protected properly. Assigning covernames to projects without going through the CTO can also lead to duplication of usage and eventually impairment of the Cover Term program itself.

Of equal importance is the fact that the definitions of these covernames are rigidly controlled. Responsibility for releasing these definitions is vested in Q4. Even the terms themselves are controlled. Lists of individual covernames cannot be acquired without first getting the approval of T5.

I urge your readers who use covernames for projects, equipments, exercises, or operations to become familiar with NSA/CSS Reg. 10-5 to insure that they comply with its requirements. If they have any questions about the procedures to follow regarding the use of covernames they can call the NSA Cover Term Officer, [redacted] on x968-8726s.

[redacted]
Chief, T511

P.L. 86-36

ON HOW THE "GAME" OF THE AGENCY COULD BE "PLAYED" (U)

by RAMÓN SANTIAGO-ÓRTIZ, G42

P.L. 86-36

In my lifetime I have watched many baseball games, played quite a number of them, and even coached a few, so my connection with the sport consists of more than just the article "The Language of Beisbol" (Cryptolog, August 1974) that I co-authored with [redacted]

As most people know, baseball has been called the national pastime of the US of A, but I strongly believe that baseball is more than just a mere game. I think it can serve as a guide to life. We have seen teams suddenly score several runs and come from 'way behind to win a game in the last of the ninth inning; from this we can learn never to give up, to constantly keep on trying. "Sure extra-base hits" suddenly become outs because some outfielder scampers a little faster, leaps a little higher, or throws a little harder than people thought he could. Teams have protracted winning streaks or lo-o-o-o-ong slumps, just the way that individuals have good days and bad days. And so on, and so on and so on.

Not surprisingly I have often thought that the "game" in the Agency for which I work should be played just like baseball too. Unlike the Agency, in baseball the guys who play on the field--the ones who produce the hits or make the catches, who slide and get their uniforms dirty, who get injured. sometimes badly--these "soldiers in the trenches" do get better salaries and greater recognition than the team managers because they do the tough, dirty work. I think that NSA should follow a similar practice.

The truth is that most of my experience has been in G Group, involved with Spanish-language problems, particularly with voice problems. But even if what I have seen and heard there is not 100% applicable to other parts of NSA, it is sufficiently widespread within G Group (which is, after all, an important part of the Agency) to warrant mention....and to justify my comments.

One way that the Agency could profit by following baseball is in the treatment of managers. A baseball skipper is praised for his team's successes and blamed for his team's failures and losses. It is not unusual for a team's owner to fire the manager when the team has lost a large number of its recent games, regardless of how many games had been won the month before. No excuses, no delays; just "get rid of the bum" and get another manager, who might do better. And, if the new guy doesn't improve the situation, fire him and get somebody else! Good performers do not need to worry!

After all, managers don't win the games; the players do. For every case where a baseball manager has made a clever game-winning change in the line-up or spotted a rule infraction that negated an opponent's advantage, you can find cases of substitutions that backfired: relief pitchers who walked in the winning run pinch hitters who struck out, etc. Why do managers, in the whole US government, no matter how "good" or "bad," seem to get most or all of the "goodies"?

I suppose that there may be a number of ineffective managers at NSA who, instead of being fired, get shifted to other managerial positions (spreading their incompetence around), sometimes even higher positions? The justification for their advancement would be the outstanding job done by the members of their "team" but, unfortunately, the "players" whom that manager supervised, the ones who turned in the outstanding performances for which the manager was rewarded, are left behind, unsung, unmentioned, unrewarded, unpromoted, etc.

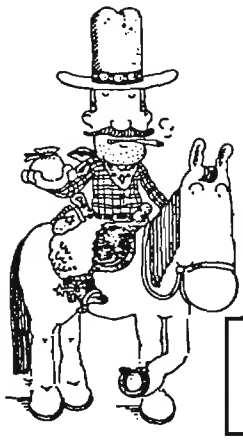
I do not claim, or even wish, that the managers in the Agency should be as good at their jobs as the analysts and technicians whom they supervise That is not their mission in the Agency unless they are "working managers" who put on a set of earphones, man a position, and get into the fray with the rest of the "troops." Only a small percentage of them do so. Once there were a few "player-managers" in baseball, but the fans didn't expect a player-manager's batting average to be the highest on the team. They did, however, expect him to contribute hits and fielding plays to help his team win games. Similarly, a working manager in an Agency voice shop may not have the keenest ear or the biggest vocabulary but he should be able to do a creditable job helping his "team" win their "big game" with his managerial skills.

It is very easy for a manager to say, "Pedro, do this!" or "Pancho, do that!"--even easier if Pedro and Pancho here at NSA, like Yaz, Pete, Reggie, and Gaylord on the ballfield, have been for many years playing the game well with minimal supervision or help from their manager.

There is a particularly great discrepancy here, though, when Pedro and Pancho, after 18 years in the Agency are still grade 12, but most of their non-linguist co-workers have gone on to greater glory. Pedro and Pancho happen to be bilingual native Spanish linguists at NSA, as is Pablo, their manager. If they were "performers" in the major leagues, their performances would have been comparable to batting .340 lifetime with a .989 fielding average and their salaries would have been increased accordingly after each successful season because in the major leagues it doesn't matter if your name is Joe Doe or Pancho Perez, just as long you hit well and field well.

There is something else that I think NSA can borrow from the national pastime. Baseball is willing to make changes, adopt innovations (e.g., the expansion of the leagues, recognition of free agent status, the designated hitter, annual rules revisions, etc). NSA should be willing to make changes too, even if only to see if such "rule revisions" might be better than the existing procedures. In the August 1977 issue of Cryptolog I wrote an article ("Telling It Like It Is") in which I pointed out some of the problems faced by the Agency's Hispanic linguists. Isn't it pathetic that now, six years later, I can write this article since very little has changed? (The only good thing that has happened to linguists in the interim is the introduction of the FLIP [Foreign Language Incentive Program] bonuses).

Former baseball player Joe Garagiola once referred to the impartiality of baseball umpires by saying something like "An umpire doesn't care if a black arm is throwing the ball past a Jewish batter's bat to an Italian catcher's mitt. He's only interested in whether the pitch is a ball or a strike." Maybe we at NSA could use a few such umpires who are concerned with the quality of the job that's being done, not with the ethnic background of the person or persons doing it...and with rewarding those who are doing their jobs really well

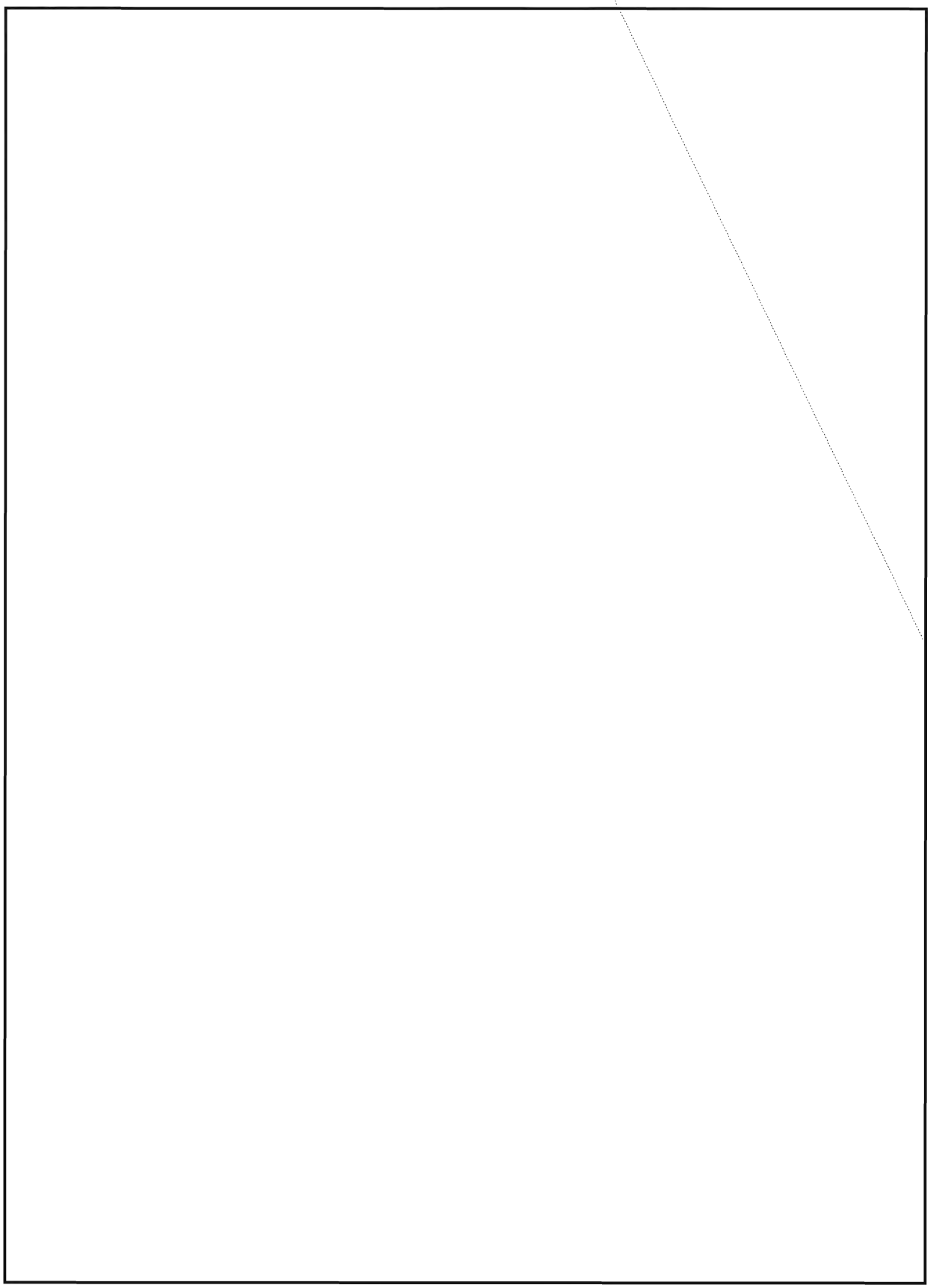


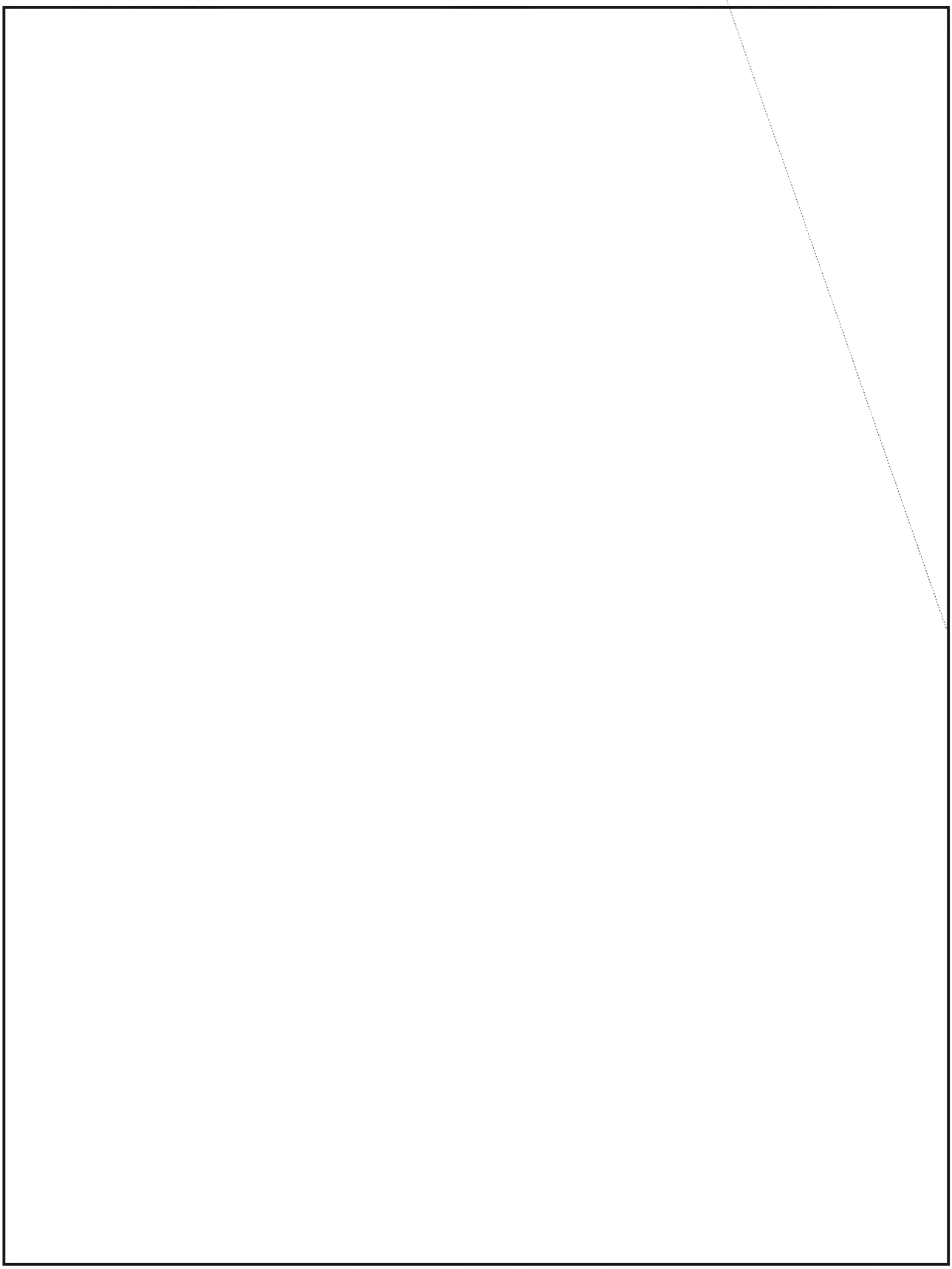
Wrangler: One Tough Customer (U)

P.L. 86-36

[redacted]

EO 1.4.(c)
P.L. 86-36





PARPRO

UNITED STATES AIR FORCE STRATEGIC AIR COMMAND'S RC-135, U-2, SR-71 RECONNAISSANCE PROGRAMS (U)

P.L. 86-36

by [redacted]
Captain, USAF JOCCP

PURPOSE

(U) This paper describes the RC-135, U-2R/TR-1, and SR-71 Peacetime Airborne Reconnaissance Program PARPRO missions from a Strategic Air Command crewmember's perspective. This viewpoint will provide insight into the capabilities and limitations of these air-breathing, airborne reconnaissance systems.

EO 1.4.(c)
P.L. 86-36

BACKGROUND

~~(S)~~ Strategic Air Command (SAC) reconnaissance programs represent the Air Force contribution to worldwide flexible SIGINT support of the intelligence community and our military commanders. With proper support, reconnaissance platforms can fly global missions on very short notice. Although initially tasked prior to overseas deployment, they have the flexibility to fulfill additional requirements once deployed. [redacted]

However, these manned reconnaissance missions provide indispensable intelligence, with the flexibility to satisfy both wartime and peacetime cryptologic needs.

~~(C)~~ Through the Strategic Reconnaissance Center (SRC) at SAC Headquarters in Omaha, Nebraska, SAC acts as the controlling authority for all USAF PARPRO operations. SAC has the responsibility for the operation and maintenance of the PARPRO airframes, while interception equipment maintenance is performed by a combination of SAC and Electronic Security Command (ESC) Personnel and civilian contractors.

~~(C)~~ The SRC coordinates proposed reconnaissance operations with the Joint Chiefs of Staff/Joint Reconnaissance Center (JCS/JRC), NSA, and theater commanders. [redacted]

~~(S)~~ The U-2/TR-1, SR-71, and RC-135, though radically different in design and capabilities, have some similarities:

- [] All are tasked with peripheral area reconnaissance of worldwide target countries;
- [] All are flown by SAC; and
- [] All airborne systems must satisfy dual requirements.

[redacted]

EO 1.4.(c)
P.L. 86-36

TYPICAL CREW COMPLEMENT

	SAC PERSONNEL		ESC PERSONNEL	
AIRCRAFT	Pilot	Maintenance		Maintenance
SR-71	1	-		-
U-2/TR-1	1	-		-
RC-135V/W	2	1		2
RC-135M	2	-		2
RC-135S	2	2		1
RC-135U	2	2		1

EO 1.4.(c)
P.L. 86-36

FIGURE 1. ~~(S)~~

OPERATIONAL BASES

PLATFORM		MOB	
SR-71		Beale AFB, CA	
U-2R/TR-1		Beale AFB, CA	
RC-135V/W		Offutt AFB, NE	
RC-135U		Offutt AFB, NE	
RC-135M		Offutt AFB, NE	
RC-135S		Eielson AFB, AK	

FIGURE 2. ~~(S)~~

~~(S-CCO)~~ A breakdown of the respective aircraft crew positions and command responsibility is shown in Figure 1. The pilots, navigators, and electronic warfare officers ("RAVENS") are all rated flying officers under SAC jurisdoction. Virtually all other crewmembers are enlisted and are assigned to ESC or SAC. Air Force Specialty Codes employed for ESC crews are 205XX (Special Signals Analysis), 207XX (Manual Morse, Radioprinter), 208XX (Linguist), and 328XX (Maintenance). All crewmembers are Category III-cleared, and selected members of the ESC crew have compartmented clearances. SR-71 and U-2R/TR-1 crews usually do not have COMINT clearances.

MISSION/AIRFRAMES

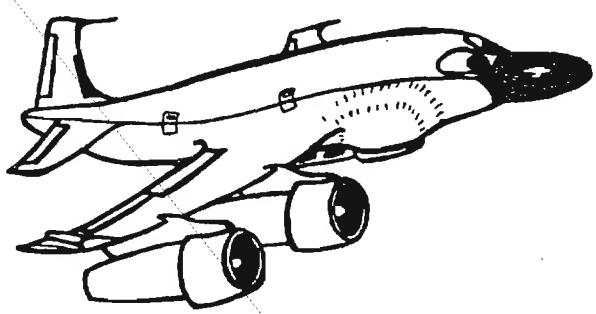
~~(S)~~ All SAC aircraft and crewmembers operate under a concept of employment involving Operating Base (MOBs) and Forward Operating Bases (FOBs). That is, training and major aircraft maintenance for all SAC reconnaissance squadrons are performed at the MOB within the US. For the U-2R/TR-1 and SR-71, the MOB is located at Beale AFB, California (9th SRW). For the RC-135S models, the MOB is Offutt AFB, Nebraska (55th SRW), and for the RC-135 it is Eielson AFB Alaska (6th SRW). From the MOB the SAC crews are deployed for 90 to 160 days per year to FOB locations. SAC RC-135M/V/W ELINT crewmembers (RAVENS) are sent to all FOB locations, and thus become qualified for all areas of the world, unlike ESC personnel, who are permanently stationed in the FOB and MOB countries and accordingly specialize in only their particular geographic area. A chart depicting the MOB and FOB locations associated with each system is found in Figure 2. Although these aircraft normally operate from the FOBs shown, they are able to deploy to many other locations on short notice. Figures 3 through 5 present specific missions and capabilities of each platform. Note that the different models of the same aircraft type have a different airframe/electronic fit (i.e., internal configuration, equipment, engines, and seat placement are different).

WHITE WOLF REVIEW

~~(S-CCO)~~ WHITE WOLF (WW) is the Advisory Support Program instituted by JCS to provide protection for PARPRO aircraft flying in or near potentially dangerous territory.

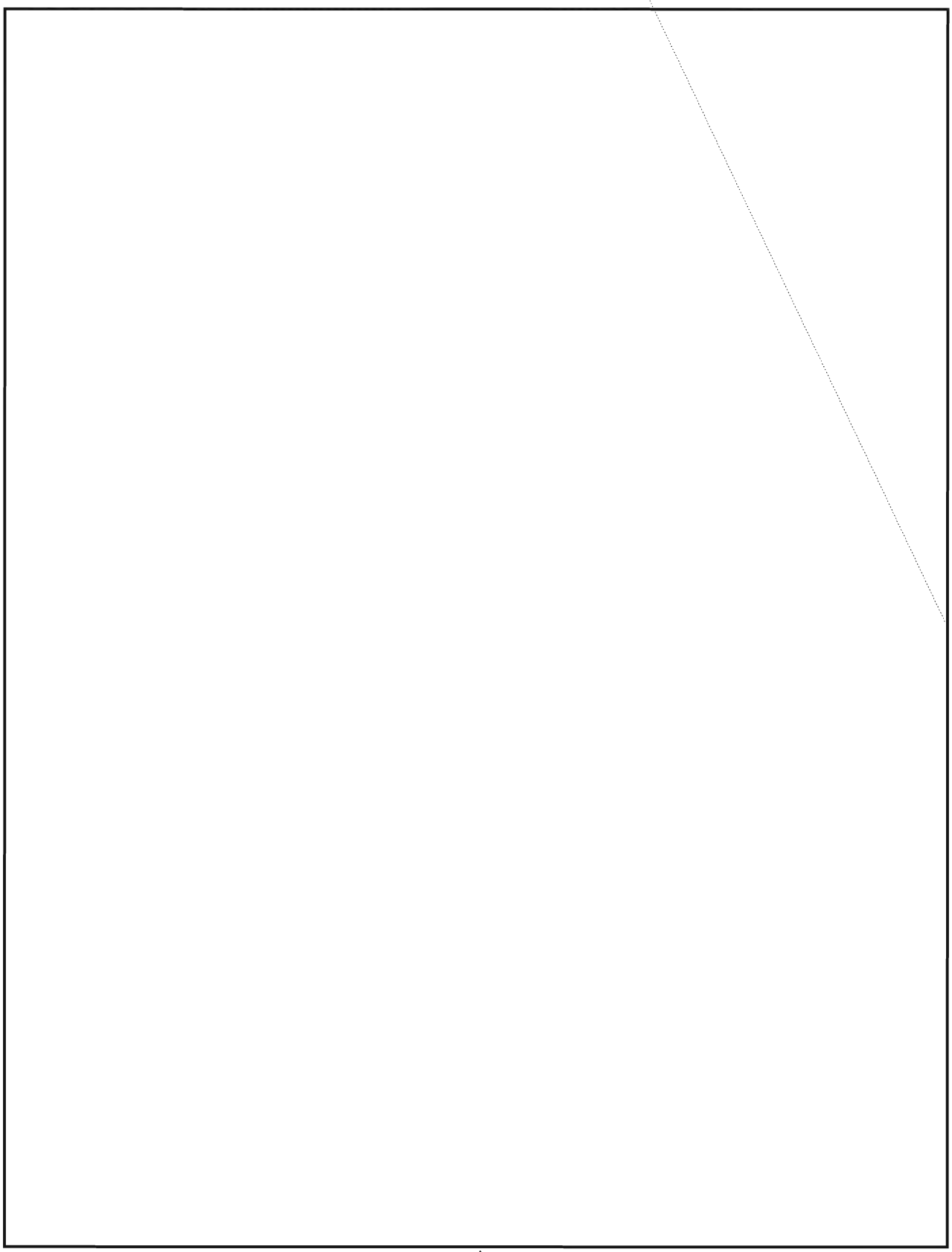
OPERATIONAL FACTORS

(U) The following information concerning factors affecting the crew is based on the author's experience and provides insight into manned ELINT collection missions. The crewmembers' duty day includes more than the actual flight time. There are five briefings and aircraft checkouts. The flight time limitation for a normal crew is 24 hours. If the crew is augmented (by adding one pilot to the crew of an RC-135) the aircraft may legally stay aloft for 30 hours. Normal mission length is 8 to 18 hours for the RC-135, 8 hours for U-2R/TR-1, and 6 hours for the SR-71. No crew may legally fly more than 125 hours a month or more than 330 hours in a 90-day period. A crew also must be provided the opportunity for 12 hours of rest between flights. These limits are set for safety and health reasons: a crew that flies in excess of 100 hours in a 10- to 30-day period can be physically exhausted by the intensity of the job and and by the physical strain induced by a noisy (120 dB) environment.



EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



(U) Extensive facilities are required to support the aircraft and crew. For example, the SR-71 requires special fuel and special airborne tankers that actually heat the fuel so that it does not turn from liquid to a gelatinous state prior to refueling. All aircraft need specialized maintenance support to include test equipment, military technicians, and civilian contractors. With the complexity of these airborne systems (sometimes one-of-a-kind equipment), quality maintenance support is sometimes difficult to attain. Insufficient spare parts is a common problem. Quarters and messing facilities have to be available for the crew and support personnel because of the MOB/FOB concept. When quarters close to the operations are not available, the additional time spent in transit to and from a base can impact on a crew's rest.

(U) The RC-135 and SR-71 usually need air refueling (i.e., tanker) support. If two tankers are required, then three crew and three tankers must be available in case one aircraft aborts. All PARPRO mission refueling tankers have a spare aircraft and crew scheduled as a backup.

(U) Weather can also be a major factor. Missions are sometimes delayed or canceled due to adverse weather. Crosswinds are a factor in the launch decision, and airfield weather visibility (e.g., due to fog) cannot be less than approximately half a mile horizontal and and 150 feet vertical. Moisture and temperature extremes frequently cause problems with complex onboard electronic equipment.

ADDITIONAL CONSIDERATIONS

(U) On the RC-135 the average time required after takeoff to turn on, check, and calibrate the equipment is 30 minutes. Often computer systems dump the program and need to be brought up several times or restarted during a mission. This occurs as a result of vibration, temperature extremes, and power fluctuations inherent in airborne platforms.

~~(C)~~ PARPRO missions may continue with degraded equipment or totally inoperative stations as long as minimum advisory support capability exists. The maintenance technicians on an RC-135 can work miracles in the air, but many times broken equipment cannot repaired due to a lack of a correct (spare) "black box" or the inaccessibility of equipment.

[redacted]

EO 1.4.(c)
P.L. 86-36

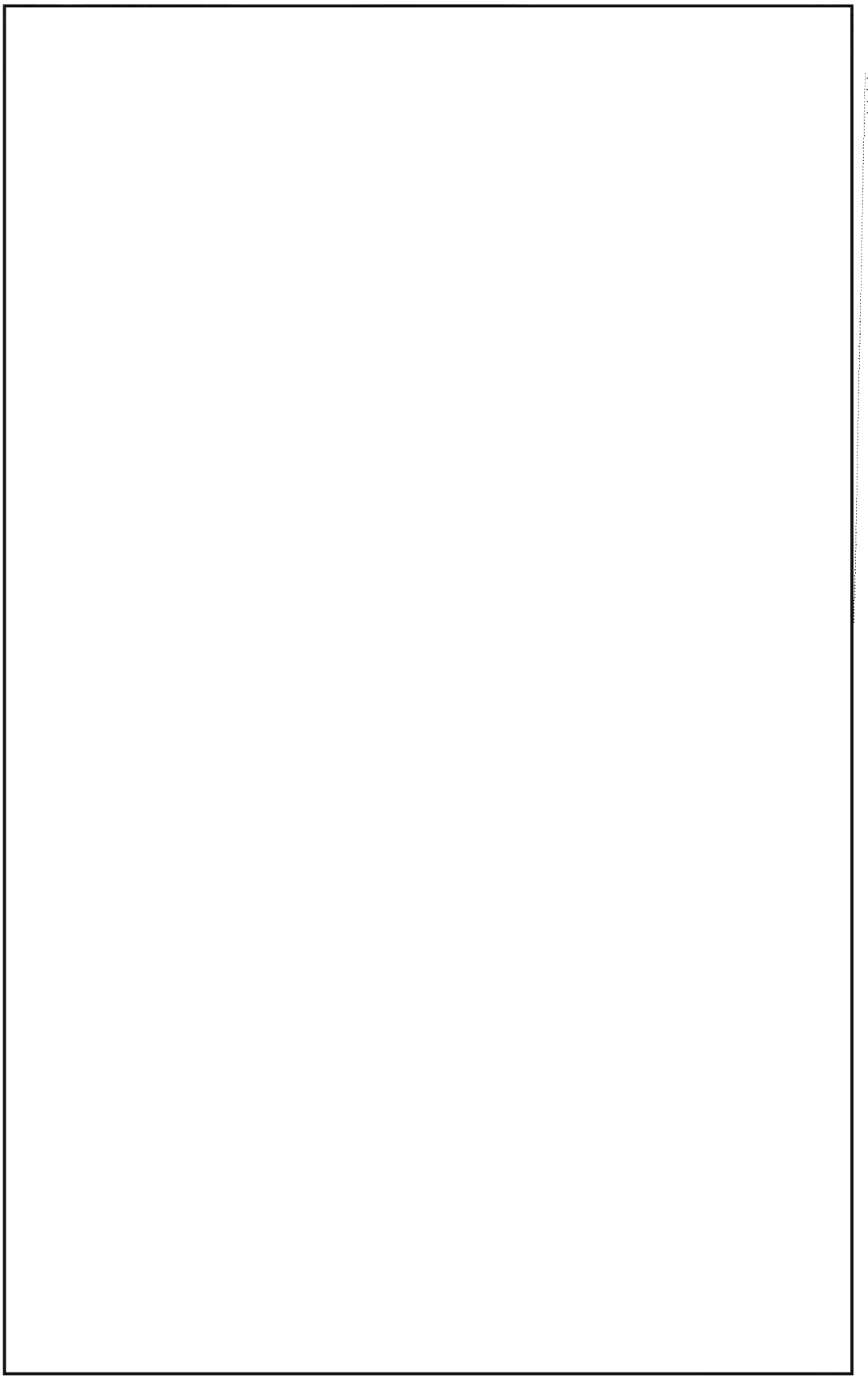
~~(SC)~~ Stress on the crew is amplified by the proximity of hostile interceptors and ground-based and shipborne weapons systems. (Hostile pilots have been known to fly as close as 10 feet to mission aircraft.) All intercepting aircraft are armed while all reconnaissance platforms, with the exception of the SR-71, are without any defensive electronic countermeasures or munitions. RC-135s do not even carry Radar Warning Receivers (RWRs). The crewmembers view the lack of an RWR with concern.

[redacted]

EO 1.4.(c)
P.L. 86-36

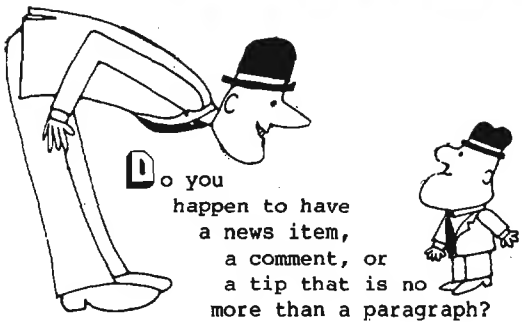
CONCLUSION

~~(C)~~ In this article I have presented some facts and opinions about PARPRO that may not be common knowledge. The missions collect intelligence in much the same way as other systems. However, the missions also have some radical differences, and the risk factor is much higher. There are many factors that affect the SAC PARPRO missions that are not present in conventional collection systems, including a lack of NSA control. Hopefully, this paper will facilitate an understanding of, and an appreciation for, the special capabilities and some of the limitations of the PARPRO missions. This additional knowledge may allow more optimum tasking and efficient management of these systems.



EO 1.4.(c)
P.L. 86-36

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph?

Or perhaps you have an article of several thousand words? Never mind how big it is! Long or short, if it has something worthwhile to say, we'll probably print it. Of course, a shorter item has a much better chance of getting read.

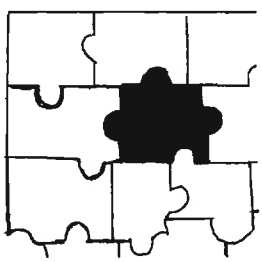
First-person articles or stories about your own experiences are welcome, so long as they relate in some way to our work.

[redacted]

EO 1.4.(c)
P.L. 86-36

Want anonymity? A thoughtful piece on a subject of interest to a fairly large number of readers will be considered for anonymous publication, if the author requests it. If you want to use a pseudonym, that is OK too....but the writer must identify himself or herself to the editor in an accompanying memo or by phone. Needless to add, a personal or trivial complaint (e.g., "My supervisor takes government paper clips home from the office") will not be considered.

Something missing? If you feel that your work or your interests are not being well represented in Cryptolog, it is probably because you and your friends are not contributing. The editors sincerely want to cover the whole territory of NSA's interests, but articles don't grow on trees, y'know! Somebody who knows the subject matter has to write them!



Your contribution does not have to be typed. We'll give preference to content over form every time. However, especially in the case of a long piece, the editorial eye will appreciate any effort you can make to get your article typed (and we'll even forgive a strikeovers and misspellings). Nowadays, of course, if you have access to a terminal connected to the Agency network, you can simply send it to us at cryptolg@bar1c05 and we can do our editing right at the terminal. But we have also accepted an item handwritten on a used lunch-bag.

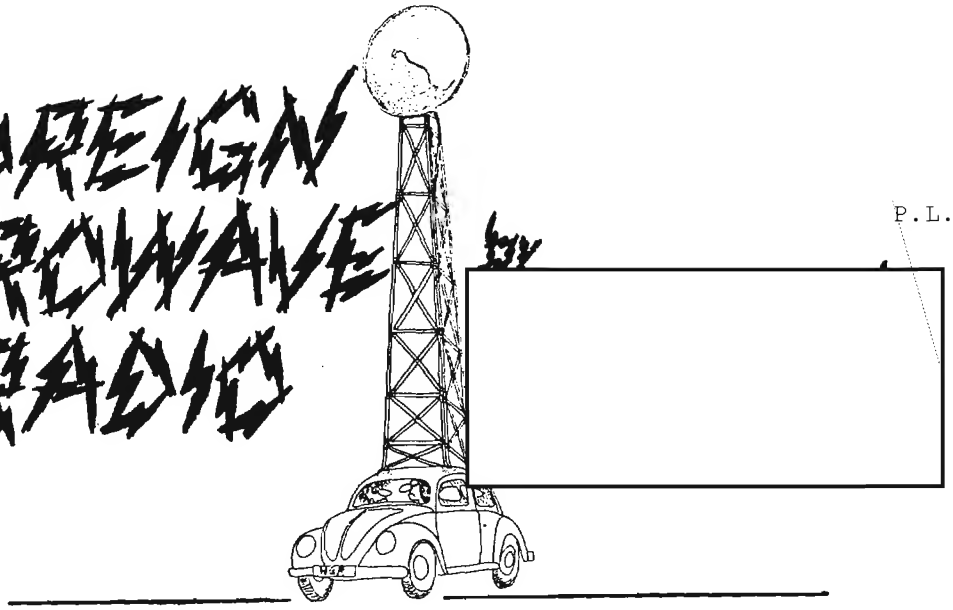
Photographic illustrations can be reproduced in Cryptolog at the same quality as in the NSA Newsletter.

Sensitive materials?? No way!!!! We'll publish articles all the way up to TOP SECRET CODEWORD, but we have to draw the line at compartmented or otherwise exclusive sources.

Need assistance? You may have a half-finished article, or an outline, or some incomplete notes, or maybe just an idea about an item you'd like to write, something you feel has possibilities but you aren't quite sure what to do with it. A quick call to the appropriate departmental editor (or the Assistant Editor, ext 1103) will probably get you the aid and comfort you need. It may even give you the inspiration to finish your magnum opus!

Our deadline? Theoretically we should have one, but we don't. After all, Cryptolog is a monthly publication, so if we get your article just after one issue has gone to press, you'll be in time for the following month's edition. There's no such thing as a bad time to submit an item to Cryptolog.

FOREIGN MICROWAVE RADIO



by

[redacted]

P.L. 86-36

(U) Hungary is the center for microwave radio technology in the Eastern Bloc, doing both R&D and production of new microwave radio equipment for Russia and the other Bloc nations, according to Dr. Ferdo Ivanek of Farinon Corp. In a recent talk to an IEEE Microwave Technology class at the University of Maryland, Dr. Ivanek showed some slides of the new 120-mm "Slimline" equipment that the Hungarians are building and remarked that they do very good work and publish their results. Journals such as Budavox and Hiradástechnika carry articles on new data, switching, and telephony systems (in Hungarian).

(U) Before World War II the Hungarians were doing advanced work in commercial radio equipment, although the Czechs were ahead in consumer electronics. Bombing and other war operations apparently did not severely damage the Hungarian industrial base so that they were able to catch up with Western developments. The Hungarians have recently developed a baseband equalization processor to correct channel distortions of microwave baseband signals, with the result that they can now transmit 1,800 voice channels over the same radio bandwidth that formerly carried a 900-channel FM signal. In their laboratories they commonly develop very modern equipment, using components and other microwave devices imported from the West or Japan. However, Dr. Ivanek pointed out, the Soviet policy of economic autarky insists that all radio production equipment must use domestically produced components which are manufactured in the Soviet Bloc. Because the Bloc nations are not able to manufacture the most modern components, a 10-year lag occurs while the manufacturing problems are being solved, and the equipment is obsolescent by the time it gets into large-scale production.

(U) The demand for autarky produces a backlog of unsatisfied needs, so that at times the USSR and its satellites must go on a "buying spree" to get vitally needed equipment. The USSR is currently buying a considerable amount of telecommunication equipment abroad. According to one comment in the class, the USSR has bought some L. M. Ericsson AXE switches and has written unusually favorable comments about these switches. Dr. Ivankek said that Tellettra, a Fiat subsidiary, had sold the USSR a large 4-GHz trans-Siberian radio relay system.

(U) The demand for autarky not only limits the market for equipment, but Dr. Ivanek expressed the strong opinion that the Soviet Bloc nations would have their own clocks and timing standards for the digital nets they were developing rather than derive timing from the Western European PTT nets.

(U) One of the implications of Dr. Ivanek's comments about the leading role of the Hungarians in this area of microwave technology is that the Hungarians may be able to sell equipment to the Western market which will later be used in the Soviet Bloc nations, after the inevitable lag in solving the manufacturing problems of producing domestic components. Further, the Hungarian literature and the appearance of the Hungarian vendors at trade shows such as Telecom 83 may give valuable information about microwave radio technology that will later appear in the USSR and other Bloc nations. A survey of some foreign technical data showed 33 papers on Hungarian microwave equipment. In addition, abstracts of Hungarian papers are available from computer data bases.

(U) The major differences, from a business point of view, between the US and the foreign

microwave radio market are, according to Dr. Ivanek:

1. Market size;
2. Equipment characteristics;
3. Monopolies vs deregulation;
4. Technical standards;
5. Domestic industrial capability; and
6. Commercial versus military applications.

(U) In market size, the once fragmented European market has caught up with the North American market, and the Asian market is expected to catch up with the North American by 1990. Latin America by 1990 will have about 30 million subscriber lines, roughly equal to the 1970 Asian market. The African and Oceanian switched public telephone plant will remain small compared to all the others. (Dr. Ivanek drew on a Telecom 79 report by Kamman et al of A. D. Little which forecast the telecom market.)

(U) Number of telephones (millions)

Year	1970	1980	1990
North America	80	110	140
Europe	50	110	210
Asia	30	60	140
Latin America	10	17	30
Oceania, Africa			10

(U) Operating Revenues (billions of 1979 $)

Year	1975	1980	1990
NA	35	67	122
Eur	26	57	164
Asia	17	38	80
LA	2	4	9
Oceania	1.6	3	4
Africa	.6	1.5	4
	81.6	171	383

(U) Shipments of Telecom Equipment (in billions of 1979 $)

	1970-80	1980-90
NA	62	103
Eur	76	196
Asia	40	59
LA	6	15
Africa	1.6	5
Oceania	3	7
	198.6	385

(U) Shipments by Equipment Type (in billions of $)

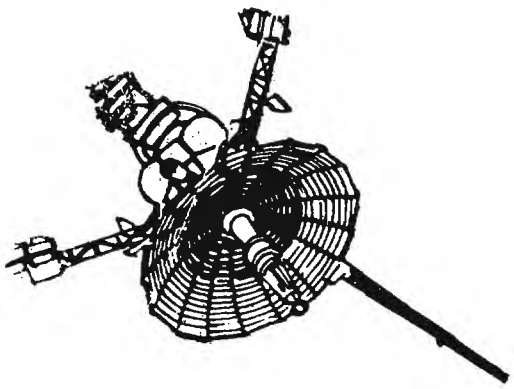
	1970-80	1980-90
C.O. switching	47	92
Long-Haul Xmsn	27	53
Local Dist.	60	117
Station Apparat.	35	68
Other	17	35
	186	365

(U) Of this extensive plant, worldwide sales of microwave radio transmitters and receivers will comprise about $10 billion per decade, or $1 billion annually (in 1979 dollars).

(U) Only a small part of the European market is open to competitive selling, because of the power of the PTTs to control telecommunication procurement and design. US industry has a lesser commitment to export sales than manufacturers in Europe and Japan. For example the exports of French microwave radio relay equipment over the past decade have been almost the same volume as the sales to the PTT, despite an intensive program of microwave installation inside France. The CNET (the French version of Bell Labs) sponsors development projects with the French companies SAT and Thompson-CSF to build the same equipment. In some product categories the two companies are given monopoly positions, while in others they compete head on. Part of the CNET microwave development plan includes equipment by SAT or Thompson CSF which is exclusively for export--there is no internal French market, yet the government, through CNET, subsidizes the development. The French government also does careful market research for telecom equipment.

(U) The German PTT (Bundespost) does not go as far as the French in sponsoring export activities but it does keep the door open for marketing of German equipment through participation in the CCIR (the International Consultative Committee of Radiocommuncations), where international standards for equipment are set in a way that helps German exports.

(U) Examples of markets developed by the French are Mexico and Brazil, which use CCITT equipment and standards and no longer follow North American standards. Latin America, Asia. Africa, Oceania, and Europe all have adopted CCITT standards. Only the US, Canada, Japan. Soth Korea, and Taiwan still use primarily North American telecom standards. This seriously limits the exports of US radio equipment, switches, digital systems, modems, and all the rest of modern telecommunication apparatus.



(U) At CCIR and WARC meetings, the US delegations, formed primarily of business people (whose technical expertise is usually much greater than that of US government officials), the US technical people are very capable in the satellite communications area and are very influential in the outcome of the conferences. In the terrestrial radio area (which is the main medium for telecommunications), the US delegations are apparently not as capable as the foreign delegations (possibly because they don't work to CCITT technical standards). Dr. Ivanek thought that the US radio industry, composed of many competing companies, needed some coordinating structure, similar to the centralized research entities that Electronic Industries Association (EIA) and Microelectronics and Computer Technology Corporation (MCC) have formed for components and microcircuitry, in order to compete more effectively in the world market.

(U) In addition to making these general observations on foreign microwave, Dr Ivanek displayed a number of slides of specific equipments from various foreign manufacturers to illustrate current developments.

(U) To begin, there was a slide of the first microwave link, developed in 1934. The British and French PTT collaborated in a cross-Channel one-hop link. It used a triode for power and operated at about 2 GHz. A parabolic antenna about 3 meters in diameter was used, predating the postwar European microwave nets by almost 20 years.

(U) A map of the French microwave network, in its current state, showed a large number of disconnected star nets. The digital trunks operate at 52, 34, 2 x 34, and 140 Mbps. These trunks connect into digital switches (which the French pioneered) into regional centers. The French are introducing digital microwave from the bottom up, on a regional basis, where the existing equipment is ready for replacement. In the Lyons area they have 2-, 8-, and 34-MBps trunks. They also have new 15-GHz nets operating at 2, 8, and 34 Mbps. They use the digital trunks to connect the E-10 digital switches. The nets are stars. There is no French equivalent of a Long Lines grid or trunk system such as AT&T uses. When the French begin to interconnect their regional centers, they will use both digital radio relay and optical fiber, according to Dr. Ivanek, since the failure modes of the two media are quite different.

(U) The UK has digital microwave nets at 140 MBps at 11 GHz. Germany has digital trunks at 2, 13, and 15 GHz. Italy has digital nets similar to the French. Switzerland has digital nets for data transmission (where the other nets are for voice or data).

(U) Analog microwave radio is still flourishing, and the Japanese have developed a 5400-channel SSB system at 6 GHz, very similar to the 6000-channel Bell System. The Germans and French are working on similar SSB systems, but have not yet introduced them.

(U) In Switzerland they have built up microwave feeder links to cable TV distribution systems. The feeder links operate at 2.5 GHz and the distribution net works at 11 and 12 GHz. The Swiss can put two independent TV baseband signals on a single radio carrier by frequency multiplexing so the distribution system is very efficient.

(U) A map of the African microwave net PANAFTEL, from the ITU, showed substantial development in subsaharan Africa. This large network had resulted from a substantial amount of ITU assistance.

(U) The development of microwave in the PRC was covered in a January 1983 issue of Microwave System News.

(U) India has been manufacturing some of its own microwave equipment, and there was slide of a portable remote satellite earth station mounted on a truck, which the Indians had developed themselves. There was a slide of some new "Slimline" 120-mm-wide racks of equipment which the Indians were manufacturing.

(U) This new Slimline equipment, pioneered 20 years ago by the Germans (to save space in switching centers and microwave terminals), is also used in Yugoslavia and Eastern Europe. The French use it widely. In the US, only two companies make Slimline. Western Electric makes a 5-inch-wide "American" Slimline series while Farinon make CCITT-specified 120-mm Slimline equipment.

(U) As the US market is opened up by deregulation, the US telecommunications companies are gradually accepting some European designs. This reverses a long trend from 1945 till now in which US microwave circuitry was exported and became the standard in most countries. There are still many US-standard microwave equipments installed and operating as analog circuits in many countries. The change to digital transmission will see CCITT equipment dominate. Some US manufacturing companies are developing CCITT versions of their existing tested equipment (e.g., the GTD 120E and GTD 1000E PABXs are being adapted to 32-channel PCM CCITT and CEPT standards.) The microwave technologies and manufacturing methods developed by the US companies have been widely adopted overseas, but the end products differ. In analog microwave systems the interface problems are not as severe because the frequency multiplexing plans are in common use by many different manufacturers. In digital microwave systems there is a great deal of product differentiation in the technical characteristics, especially among competing US manufacturers, so that digital interfaces are more difficult to handle.

(U) US users of high powered microwave transmitters depend on foreign suppliers of TWTs (traveling wave tubes), e.g., Siemens and Thompson CSF. The TWTs are smaller and much more efficient than arrays of solid state power amplifiers; e.g., the solid state unit would consume 100 watts of power to radiate 10 watts, while a TWT would need only 20 watts to radiate 10 watts. The extra power must be dissipated as heat, and in space applications power limitations are also critical.

(U) US users of GaAs (Gallium Arsenide) components must also depend on foreign suppliers, particularly Japan. The GaAs FET (Field Effect Transistors) are crucial to microwave receiver designs and other analog microcircuits. Western Electric produces its own GaAs FETs but the other US users must obtain their components from Japan because WE has not put its components on the commercial market.

(U) Technical standards play a central role in the development and sale of microwave equipment. The CCIR is the principal agency for setting radio standards. It is slow but effective. There is no voting in the CCIR and decisions are arrived at by consensus, so that persuasion by technical representatives of the various countries is the method used to get decisions. The Japanese, who are major producers of advanced microwave equipment, are very active in the CCIR. The CCIR studies in microwave began in 1948 in Sweden. In 1951 in Germany a study on wideband radio relay, for TV distribution, was undertaken. Successive CCIR meetings in London in 1953 and Warsaw in 1956 continued this work. The main purpose of terrestrial microwave in Europe (and the US) at first was the distribution of TV broadcasting. The wideband microwave systems predated wideband tape recorders, so central studios could transmit over a network to local VHF broadcasting stations. Multichannel telephony came later, as filters and other components were developed. The USSR, although a CCIR member, would never agree to 5-MHz baseband for wideband TV transmission and, as a result, the TV baseband in COMECON is 6 MHz. This apparently was to prevent any TV interfaces between Western and Eastern Europe, according to Dr. Ivanek.

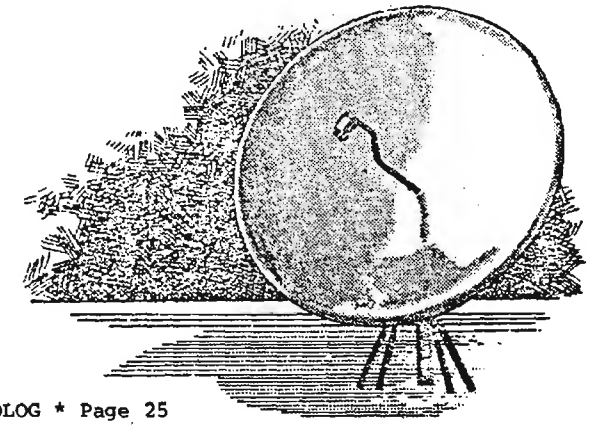
(U) Among operating microwave systems, the Japanese 400-Mbps system at 20 GHz is the highest capacity digital system in use, while the Western Electric 6000-channel AR6 is the highest capacity analog system in use.

(U) The very high efficiency of the SSB analog systems could have a significant effect on communication satellites, which are widely expected to become "all digital" by 2000. Because of bandwidth limitations in the lower microwave frequencies (under 10 GHz), the SSB analog FDM systems may be much more efficient than digital systems for most telephony.

(U) India, which lost an INSAT satellite recently, is preparing a ground station network in anticipation of a future satellite.

(U) Brazil, according to Dr. Ivanek, has serious intentions for a major domestic satellite program, using several satellites under its own operational control.

(U) AEG Telefunken has developed an 11/14 GHz (i.e., 11-12 GHz and 14-15 GHz bands for satellite transmission) regenerative repeater for digital microwave. This eliminates the need to demodulate the radio signal to an IF (intermediate frequency). This will allow onboard baseband switching on a satellite. The system is designed to operate at 120 Mbps differential QPSK (4-phase shift keying) demodulation. The hardware already exists.



(U) In France the CNET uses SAW (Surface Acoustic Wave) devices in satellite communications, for filters, digital modulators, up converters, down converters, demodulators and receiving filters. The SAW circuits are very compact, about the size of a 1-franc coin, and the link operates at 2 Mbps.

(U) In Japan a commercial satellite uses spread spectrum for two voice channels. The PN (pseudo noise) code is generated by an 8-stage register at 16.6 Mbps which transmits an information band of 65 Kbps. The Japanese also use spread spectrum for equatorial communications.

(U) An SR system in Canada uses an analog PPM TDM system at 1.5 GHz for rural communications. The system can accommodate 120 subscribers. The terminal units and transceivers are hung on a pole at the subscribers' premises.

(U) In France at Thezillieu an IRT 1500 TDMA system at 1.5 GHz is in use. The IRT 1500 (Integrated Rural Telephone) systems uses FSK for 832-Kbps transmission to 128 subscribers at 63 stations. Hops as long as 40 Km are in use.

(U) The Japanese NTT has developed a microwave overlay system that consists of a rooftop or desktop 26-GHz microwave system. The desktop model has a telephone and a shiny 12-inch parabolic antenna that sits on a desk or table. The radio links will operate over 7-Km hops at 2 Mbps. A voice channel over the radio link uses 64 Kbps per subscriber. The transmission power is 27 dBm, and the frequency stability is 0.0001. Modulation is DFSK and the system will carry 100 channels. NEC is to produce this new system. The purpose of the desktop 26-GHz system is to provide an urban area overlay system which will allow office computers and desktop computers to interconnect between tall buildings. The existing twisted pair cable systems will not carry the high data rate, so the microwave equipment allows dedicated nets to overlay the civil plant. The Japanese have tested the system and are confident that it will operate reliably through the rainy environment in Japan. This implies that the 26-GHz digital desktop microwave system will work almost anywhere in an urban area. and will allow dedicated digital nets to be set up in any city without waiting for improvements in the existing public networks. There is even a portable voice channel service set, so that a technician can test a new or existing station without using the fixed equipment. This should be a very flexible modern system, especially for dedicated nets.

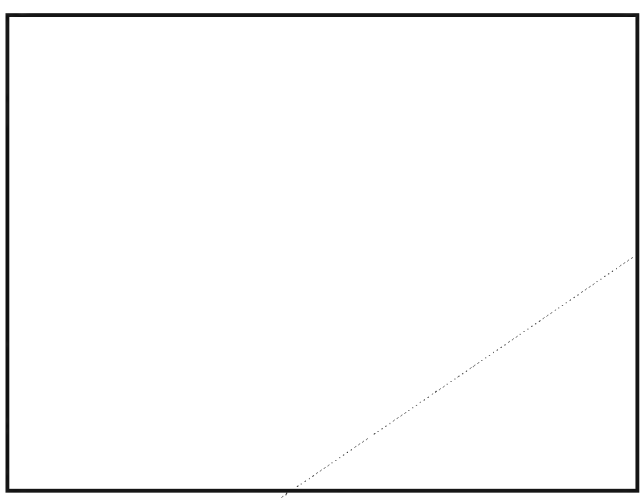
(U) Summing up, the foreign developments in microwave are as good technically as modern US equipment. Some of the new foreign systems are very well designed from a marketing standpoint. The spread of CCITT standards to almost every nation except the US and Canada gives the foreign microwave manufacturers much easier access to the world market. The US companies have been sluggish in responding to this technologic and regulatory change.

Analysis

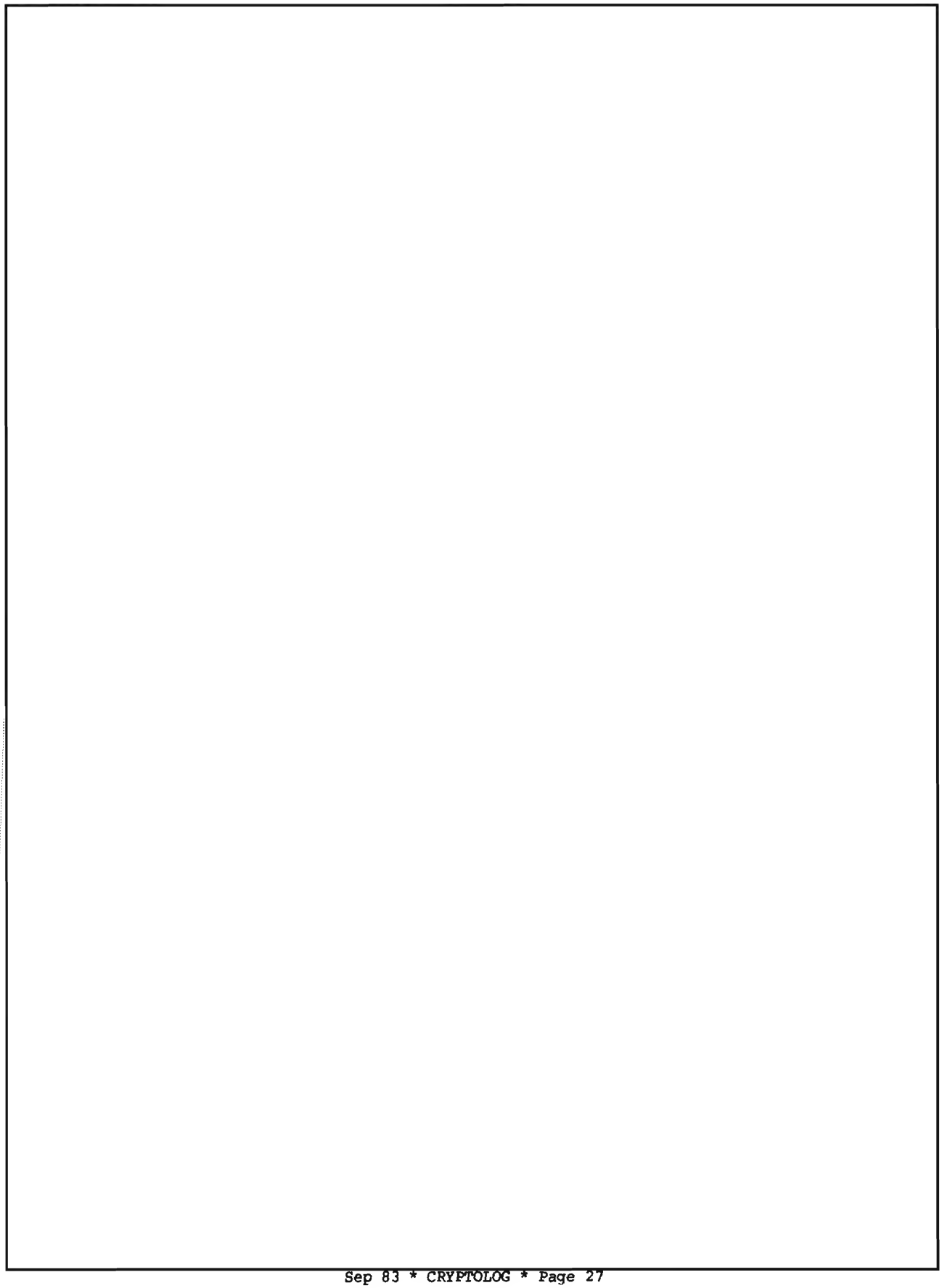
(U) Hungarian equipment and technical literature could be a fruitful source of information about microwave systems which will be used in COMECON. The apparent 10-year lag time in developing the component manufacturing capability would give some lead time for the development of SIGINT systems to deal with the new microwave technology. In addition, export control policies could be designed to lengthen the lag time for COMECON manufacture and use by blocking access to the manufacturing technology for critical components used by the Hungarians in their development models. The Hungarians may also be concerned with digital switching and protocols since the digital microwave must interface into the switches.

(U) The possibilities of the Hungarian telecommunications industry as a bellwether of Soviet telecommunications could be explored by literature searches, interviews with Dr. Ivanek, and various conventional methods of gathering information.

(U) The expected massive growth of telephony in Europe and Asia points to fruitful SIGINT opportunities. The telephone growth will be directly related to rapid economic growth in those areas. The substantial spending on local distribution ($117 billion) during 1980-90 implies that the local nets will be valuable access points for SIGINT.



EO 1.4.(c)
P.L. 86-36



NSA-Crostic #50

Here's one in the cryptic vein

A. Bethlehem, before it became a big city (2 wds)

5 18 100 68 128 79 28 137 71 177

B. Scopes trial movie is whither I intend to go (3 wds)

105 89 114 9 186 160 39 19 147 56 144 22

112 132

C. For no reason he brought needles, sly dog

121 20 47 182 127 151 108 145 12 25

D. Is he crabby? Why no, just a whiner

97 63 57 165 54 32 183

E. Judy Garland's best-known song (2 wds foll. by Word U)

155 46 152 173 133 185 111

F. Light up for prospector's fortunate find (2 wds)

30 156 51 74 33 35 146 159 176 150 24

G. Cranny leader

37 106 67 31

H. "_____ of Texas" (4 wds)

96 70 41 153 50 163 104 15 189 110 77 122

157 136

I. Death row inmate anticipates Toffler book (2 wds)

169 34 113 174 17 3 76 40 180 117 23

J. Fall of a Mau Mau nut

130 59 123 75 53 107

K. Are inflexible prigs uncommon? I say yes

1 92 43 49 149 184 181 98 119 13 81 162

8 178

L. Castle bird

87 72 118 55

M. Australian server

115 48 143 99 10 135

N. Why do you brag at a large turnip?

166 27 161 187 64 29 11 126

O. See hopes for African tomb-builder

103 134 148 82 86 2

P. For you plus me it can be rash

141 124 78 91 188

Q. Palindromic body part

139 116 120

R. Ida ran a hotel off the coast of Ireland

102 73 94 131

S. Familiar thoroughfare for Bob, Bing and Dottie

80 90 140 66

T. Interrogative

179 69 171

U. See Word E

101 6 45 83 170 88 16

V. Intravenous feeding at Harvard or Yale?

36 61 129

W. Bring back lonely tea bag for headache

44 154 21 168 175 58 85

X. Mica is in glasses or cups

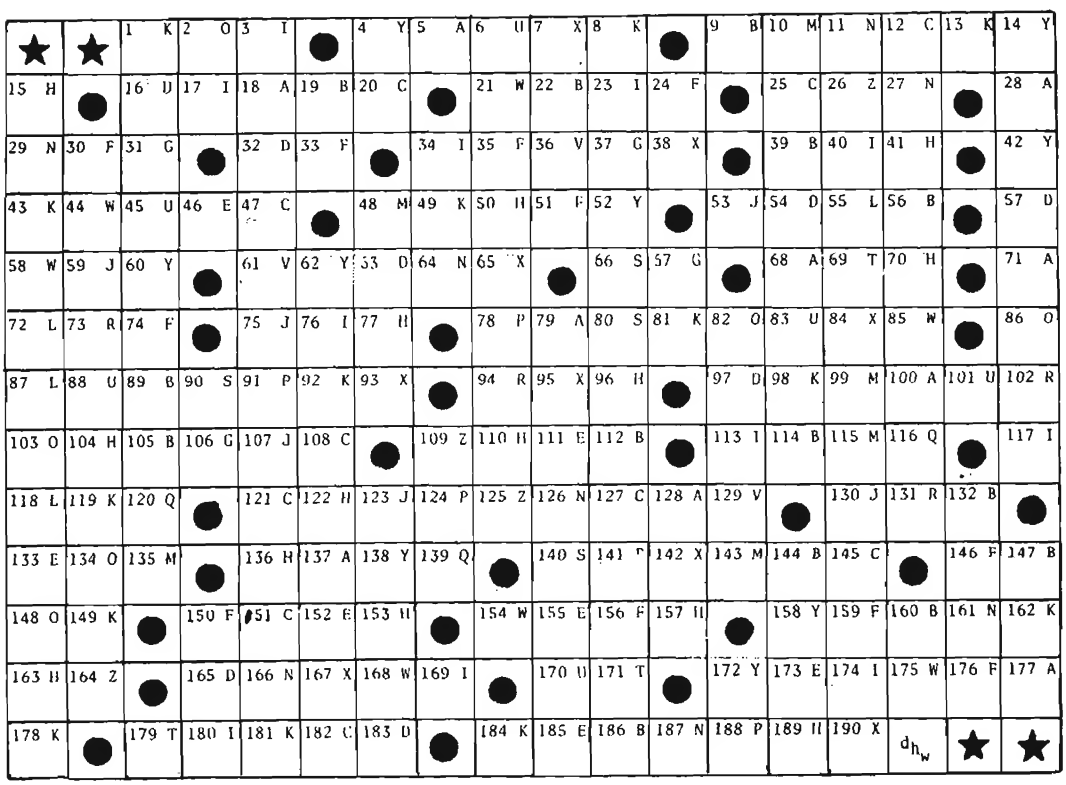
167 190 7 95 38 142 84 65 93

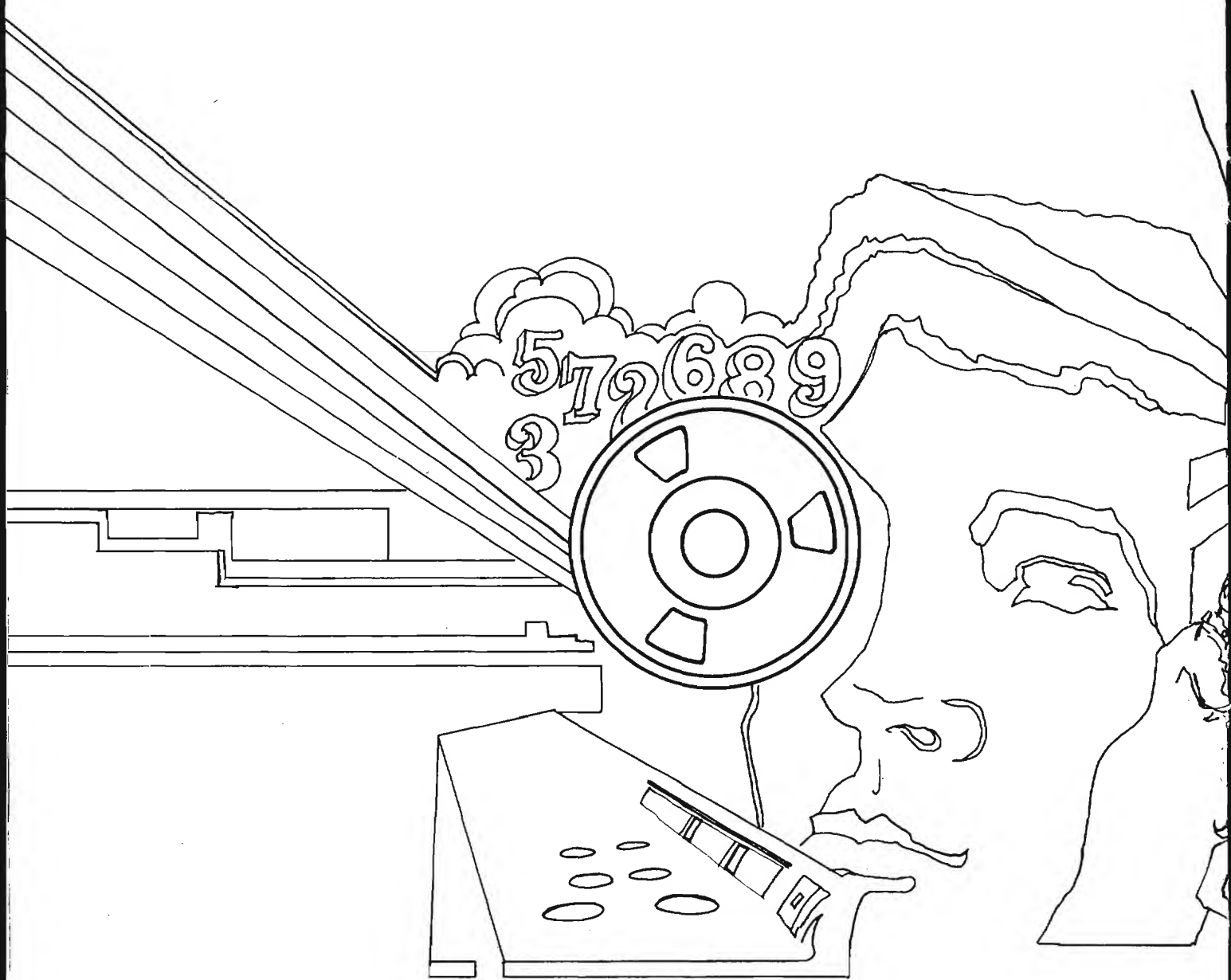
Y. Renew spa personnel's *Times* subscription

138 52 158 14 4 42 172 62 60

Z. Develop tier between F and H

164 125 26 109




5 7 9 6 8 9
3